(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 759 833**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 01965**

(51) Int Cl^6 : **H 04 L 9/14**, G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 19.02.97.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 21.08.98 Bulletin 98/34.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS* — FR.

(72) **Inventeur(s)** : WOJCIECHOWSKI REGINE, LISIMAQUE GILLES et ORUS HERVE.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** :

(54) PROCEDE DE PROTECTION D'UNE CLE MERE DESTINEE A PERMETTRE L'AUTHENTIFICATION DE CARTES UTILISATEURS.

(57) La présente invention se rapporte à un procédé de protection d'une clé mère (KM_1) destinée à permettre l'authentification de cartes utilisateurs par un lecteur comprenant un module de sécurité (SAM) . Ce procédé est caractérisé en ce qu'

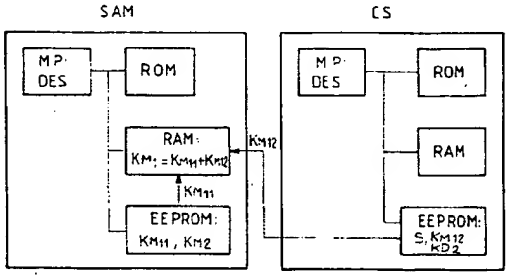
une première partie de la clé mère (KM_{11}) est stockée dans une mémoire du module de sécurité (SAM),

une deuxième partie de la clé mère (KM_{12}) est stockée dans une mémoire d'une carte superviseur (CS),

et en ce qu'

une copie temporaire de la deuxième partie de la clé mère (KM_{12}) est apportée par la carte superviseur (CS) dans une mémoire du module de sécurité (SAM) .

L'invention s'applique notamment à des systèmes fermés comme les caisses d'un grand magasin ou les machines de jeu d'un casino par exemple.



FR 2 759 833 - A1

1

PROCÉDÉ DE PROTECTION D'UNE CLÉ MERE DESTINÉE A PERMETTRE L'AUTHENTIFICATION DE CARTES UTILISATEURS

La présente invention se rapporte aux applications d'authentification de cartes utilisateurs. Elle se rapporte plus particulièrement à un procédé de protection d'une clé mère destinée à permettre l'authentification de cartes utilisateurs par un lecteur comprenant un module de sécurité.

Pour sécuriser une application, il est courant aujourd'hui d'utiliser un module de sécurité SAM (Security Application Module) placé dans un lecteur de carte. Ce module de sécurité SAM possède, dans une zone considérée comme protégée, une "clé mère" constituant la base de toute la sécurité de l'application.

Cette clé mère est programmée dans une zone mémoire du module de sécurité, lors de la fabrication ou de la personnalisation de ce dernier. Une fois cette clé écrite, l'accès à la zone mémoire est généralement verrouillé vis à vis de l'extérieur du circuit aussi bien en écriture, en mise à jour et en lecture. La mémoire dans laquelle est enregistrée cette clé mère est en général une mémoire électriquement programmable de type EEPROM.

La figure 1 schématise un module de sécurité SAM classique et une carte utilisateur CU. Le module de sécurité SAM possède un microprocesseur MP permettant de mettre en oeuvre un algorithme de cryptage par exemple l'algorithme DES (Data Encryption Security), une mémoire morte de type ROM, une mémoire volatile de travail de type RAM, et une mémoire électriquement programmable de type EEPROM. La clé mère KM, permettant

la mise en oeuvre du protocole d'authentification, est stockée dans la mémoire électriquement programmable de type EEPROM.

La carte utilisateur CU comporte elle aussi un microprocesseur MP permettant de mettre en oeuvre l'algorithme de cryptage DES, une mémoire morte de type ROM, une mémoire volatile de travail de type RAM et une mémoire électriquement programmable de type PROM ou EEPROM. Le numéro de série S de la carte utilisateur CU et une valeur KD, correspondant à une diversification de la clé mère KM, sont stockés dans la mémoire de type PROM ou EEPROM. Cette mémoire de type PROM ou EEPROM est verrouillée en écriture, en mise à jour et en lecture au moyen d'un fusible par exemple.

Ainsi, lorsque la carte utilisateur CU est insérée dans un lecteur, elle transmet au module de sécurité SAM, son numéro de série S par exemple. A partir de ce numéro S et de la clé mère KM, le module de sécurité met en oeuvre l'algorithme de cryptage DES et calcule une valeur KD' correspondant à une diversification de la clé mère KM, selon l'équation suivante : KD'=DES(S,KM).

Par ailleurs, le module de sécurité génère un nombre aléatoire, dénommé ALEA1. La valeur de l'ALEA1 est transmise à la carte CU. La carte CU génère elle aussi un autre nombre aléatoire dénommé ALEA2 et calcule, à partir des valeurs de KD et de l'ALEA2, une clé de cession Kf, encore dénommée clé fille. Ce calcul de la clé fille se fait au moyen de l'algorithme de cryptage DES, selon l'équation suivante : Kf=DES(ALEA2,KD). Puis, à partir de cette clé de cession Kf et de l'ALEA1 transmis par le module de sécurité SAM, la carte calcule une valeur intermédiaire

R, au moyen de l'algorythme de cryptage DES, selon l'équation R=DES(ALEA1,Kf).

La valeur R ainsi calculée et l'ALEA2 généré par la carte CU sont ensuite transmis au module de sécurité. Le module SAM calcule, de la même manière, une autre clé de cession Kf'=DES(ALEA2,KD') et une autre valeur R'=DES(ALEA1,Kf'), puis il compare les deux valeurs R et R'.

Si ces valeurs sont identiques, la carte CU est authentifiée et autorisée à échanger des données avec le lecteur. En revanche, si ces deux valeurs sont différentes, la carte CU n'est pas authentifiée et aucun dialogue n'est possible avec le lecteur.

La clé mère KM permet donc de mettre en oeuvre un protocole d'authentification de cartes utilisateurs pour sécuriser une application. Par conséquent, la sécurité d'une application repose sur l'inviolabilité de la clé mère stockée dans le module de sécurité SAM.

Certaines publications annoncent pouvoir récupérer frauduleusement la clé mère par une analyse cryptographique, ou par une attaque physique du module ou par tout autre moyen.

Ainsi, en inondant le lecteur de données connues, au moyen d'une carte utilisateur quelconque, il est théoriquement possible, après un grand nombre d'essais, de retrouver la clé mère à partir des messages renvoyés du lecteur vers la carte et codés par cette clé. Dans tous les cas, pour pouvoir accéder à cette clé mère, le module de sécurité doit nécessairement être arraché du lecteur et par conséquent mis hors tension.

La présente invention permet de résoudre le problème exposé ci-dessus. En effet, pour éviter qu'une attaque sur le module de sécurité permette de récupérer la clé mère, celle-ci est avantageusement partagée en

deux parties stockées sur des supports de mémorisation physiquement et géographiquement distincts. Avantageusement une première partie est stockée dans une mémoire du module de sécurité tandis que la deuxième partie est stockée dans une carte à puce détenue par une personne habilitée, et dénommée par la suite carte superviseur.

La carte superviseur permet d'apporter la deuxième partie de la clé mère et ainsi de déverrouiller les fonctions cryptographiques du module de sécurité.

La présente invention se rapporte plus particulièrement à un procédé de protection d'une clé mère destinée à permettre l'authentification de cartes utilisateurs par un lecteur comprenant un module de sécurité, caractérisé en ce qu'

- une première partie de la clé mère est stockée dans une mémoire du module de sécurité,

- une deuxième partie de la clé mère (KM_{12}) est stockée dans un support de mémorisation physiquement et géographiquement distinct (CS),

et en ce qu'

- une copie temporaire de la deuxième partie de la clé mère est apportée par la carte superviseur dans une mémoire du module de sécurité.

Le support de mémorisation détenant la deuxième partie de la clé mère est une carte à puce superviseur.

De manière avantageuse, la première partie de la clé mère est stockée dans une mémoire électriquement programmable, de type EEPROM, du module de sécurité et recopiée dans une mémoire volatile de type RAM dudit module de sécurité.

De même, la deuxième partie de la clé mère est stockée et protégée dans une mémoire électriquement programmable, de type EEPROM, de la carte superviseur

et sa copie est apportée dans une mémoire volatile de travail, de type RAM, du module de sécurité.

Selon une autre caractéristique de l'invention, la totalité de la clé mère est recomposée et stockée dans la mémoire volatile, de type RAM, du module de sécurité.

Par exemple, la clé mère est recomposée sur 8 ou 16 octets.

Enfin, la copie de la deuxième partie de la clé mère peut être apportée dans la mémoire du module de sécurité sous forme cryptée.

Le reste des opérations d'authentification se fait de manière classique, à partir de la clé mère totale recomposée et stockée dans une mémoire de type RAM du module de sécurité. Le fait que cette clé soit stockée dans la RAM permet de la protéger contre toute tentative de récupération puisqu'elle est détruite dès que le module de sécurité est mis hors tension.

Pour augmenter la sécurité, on procédera au préalable à une authentification de la carte superviseur. Une deuxième clé mère est stockée, en totalité, dans une mémoire du module de sécurité, de manière à permettre l'authentification de cette carte superviseur. De préférence, cette deuxième clé mère est stockée dans une mémoire électriquement programmable, de type EEPROM du module de sécurité.

Cette deuxième clé mère ne permet l'authentification que d'un seul type de carte : la carte superviseur. Elle ne peut donc pas être récupérée au moyen d'une carte quelconque comme la première clé mère.

Grâce au procédé selon l'invention, deux obstacles s'opposent donc à toute tentative de récupération de la

clé mère destinée à permettre l'authentification de cartes utilisateurs.

Le premier obstacle réside dans le fait que la clé mère est partagée en deux parties stockées sur des supports de mémorisation protégés, physiquement et géographiquement distincts dont un est une carte à puce "spécifique". Par conséquent, pour pouvoir reconstituer la totalité de la clé il faut tout d'abord avoir accès à cette carte "spécifique".

Le deuxième obstacle réside dans le fait que la clé mère, une fois reconstituée, est stockée temporairement dans le module de sécurité, avantageusement dans une de ses mémoires volatiles de manière à ce qu'elle puisse être détruite dès que le module de sécurité est mis hors tension.

Le procédé selon l'invention s'applique notamment à des systèmes fermés tels que les caisses d'un grand magasin ou alors les machines de jeu d'un casino par exemple.

D'autres particularités et avantages de l'invention apparaîtront à la lecture de la description faite à titre d'exemple non limitatif, en référence aux figures annexées qui représentent :

- la figure 1, déjà décrite, un schéma d'un module de sécurité classique et d'une carte utilisateur,
- la figure 2, un schéma d'un module de sécurité et d'une carte superviseur utilisés pour la mise en oeuvre du procédé selon l'invention,
- la figure 3, un organigramme d'un protocole d'authentification d'une carte utilisateur mettant en oeuvre le procédé selon l'invention.

Le schéma de la figure 2 permet de comprendre la manière dont la clé mère KM_1, destinée à permettre

l'authentification de cartes utilisateurs quelconques, est stockée, après sa recomposition, dans le module de sécurité SAM.

Le module de sécurité SAM est de type classique : il comprend un microprocesseur MP, une mémoire morte de type ROM, une mémoire volatile de travail de type RAM, et une mémoire électriquement programmable de type EEPROM. Le microprocesseur MP permet de mettre en oeuvre un algorithme de cryptage comme par exemple l'algorithme DES.

De préférence une clé mère KM_2 destinée à authentifier une carte spécifique, dite superviseur CS, est stockée dans la mémoire électriquement programmable et à accès protégé, de manière à ce qu'elle ne soit accessible ni en lecture ni en écriture. Cette clé mère KM_2 n'est destinée à authentifier qu'une seule carte si bien que son accès n'est pas intéressant pour un éventuel fraudeur. En effet, la clé susceptible d'intéresser un fraudeur est celle qui permet d'authentifier une carte utilisateur quelconque afin de pouvoir accéder à certaines applications.

De manière avantageuse, une telle clé, référencée KM_1 sur la figure 2, est partagée en deux parties, entre le module de sécurité SAM et la carte superviseur CS. Par conséquent, pour pouvoir recomposer la totalité de la clé mère KM_1, il faut, dans un premier temps, avoir accès à la carte superviseur CS.

La carte superviseur CS comprend, tout comme une carte classique, un microprocesseur MP permettant de mettre en oeuvre un algorithme de cryptage DES, une mémoire morte de type ROM, une mémoire volatile de travail de type RAM et une mémoire électriquement programmable de type EEPROM. De préférence, un numéro de série S et une valeur KD2, correspondant à une

diversification de la clé mère KM2 d'authentification de la carte superviseur CS, sont stockés dans la mémoire électriquement programmable EEPROM de cette carte superviseur CS.

De manière avantageuse, la clé mère KM_1 destinée à authentifier des cartes utilisateurs est partagée entre le module SAM et la carte superviseur CS. De préférence, une première partie de cette clé KM_{11} est stockée dans la mémoire électriquement programmable EEPROM du module de sécurité SAM tandis que la deuxième partie de cette clé KM_{12} est stockée dans la mémoire électriquement programmable EEPROM de la carte superviseur CS.

Ainsi, lorsque la carte superviseur CS est insérée dans un lecteur, et qu'elle est habilitée à dialoguer avec lui, elle apporte au module de sécurité SAM de ce lecteur une copie temporaire de la deuxième partie KM_{12} manquante de la clé.

De préférence, la copie de la deuxième partie de la clé KM_{12} est apportée dans la mémoire volatile de travail de type RAM du module de sécurité. De la même manière, la première partie de la clé mère KM_{11} est recopiée dans la mémoire volatile de travail RAM du module de sécurité, afin de pouvoir recomposer la totalité de cette clé KM_1.

La totalité de la clé mère KM_1 est de préférence reconstituée sur 8 ou 16 octets. Bien sûr, dans une variante de réalisation, cette clé peut être recomposée sur plus ou moins d'octets.

Selon une autre variante de réalisation il est en outre possible que la copie temporaire de la deuxième partie de la clé mère KM_{12} soit apportée sous forme cryptée dans la mémoire du module de sécurité SAM, de

manière à éviter qu'elle ne soit interceptée lors de son transfert vers le module de sécurité.

Le fait de stocker la clé mère KM_1 dans une mémoire volatile de type RAM permet de la protéger contre toute tentative de récupération puisqu'elle est détruite dès que le module de sécurité est mis hors tension.

De plus, on peut imaginer que le microprocesseur MP du module de sécurité détruise la clé dès qu'il détecte une attaque quelconque du module SAM, c'est à dire avant la mise hors tension.

Ainsi, même si le premier obstacle à la récupération de la clé mère a été franchi, à savoir l'accès à la carte CS, un deuxième obstacle subsiste : la destruction de la clé lors de la mise hors tension du module SAM.

L'organigramme de la figure 3 schématise un protocole d'authentification d'une carte utilisateur CUn quelconque mettant en oeuvre le procédé de protection de la clé mère KM_1 selon l'invention.

Ce protocole d'authentification comprend trois phases distinctes. La première phase, référencée 100 sur la figure 3, correspond à l'authentification d'une carte superviseur CS ; la deuxième phase, référencée 200 sur la figure 3, correspond à la recomposition de la clé mère KM_1 destinée à permettre la réalisation de la troisième phase, référencée 300, à savoir l'authentification d'une carte utilisateur quelconque CUn.

L'authentification de la carte superviseur CS (référence 100) est réalisée selon une procédure classique telle que décrite précédemment. Cette procédure est à nouveau brièvement expliquée au regard de la figure 3. La carte superviseur transmet son

numéro de série S au module de sécurité SAM de manière à ce que ce dernier puisse calculer une valeur KD_2' de diversification de la clé mère KM_2 correspondante. Cette valeur KD'_2 est calculée à partir de S et KM_2, au moyen de l'algorithme de cryptage DES (c'est l'étape 110). Une valeur correspondante KD de diversification de la clé mère KM2 est par ailleurs stockée dans une mémoire de la carte CS.

Le module de sécurité SAM et la carte CS génèrent chacun un nombre aléatoire, respectivement ALEA1 et ALEA2 (étapes 120 et 121). Les valeurs des ALEA1 et ALEA2 sont respectivement transmises à la carte CS et au module SAM (étapes 120 et 131).

La carte CS d'une part et le module SAM d'autre part calculent chacun une clé fille, ou clé de cession, notée respectivement Kf_2 et Kf'_2 à partir des valeurs KD_2, KD'_2 et de l'ALEA2, au moyen de l'algorithme de cryptage DES (ce sont les étapes 130 et 140). Des valeurs intermédiaires R_2 et R'_2 sont ensuites calculées respectivement par la carte CS et le module de sécurité SAM, à partir de l'ALEA1 et des clés filles Kf_2, Kf'_2 (étapes 131, 141). La valeur R_2 calculée par la carte CS est transmise au module SAM et comparée à la valeur intermédiaire R'_2 calculée par ce module (c'est l'étape 150). Cette comparaison est effectuée par le module SAM.

Si ces deux valeurs sont différentes, la carte n'est pas authentifiée, elle ne peut donc pas donner l'habilitation pour procéder à l'authentification des cartes utilisateurs, c'est à dire qu'elle ne peut être utilisée en tant que carte superviseur.

En revanche, lorsque les deux valeurs sont identiques, alors la procédure d'authentification d'une carte utilisateur CUn peut commencer. Pour cela, la clé

mère correspondante KM_1 doit être recomposée temporairement à partir de la première partie KM_{11} stockée en mémoire du module SAM et de la copie de la deuxième partie KM_{12} manquante apportée en mémoire du module de sécurité SAM par la carte superviseur CS (c'est l'étape 200).

La copie de cette deuxième partie KM_{12} de clé est par exemple apportée sous forme cryptée de manière à éviter qu'elle ne soit interceptée lors de son transfert. La clé KM_1 est de préférence recomposée dans la mémoire RAM du module SAM.

La procédure d'authentification 300 d'une carte utilisateur CUn, à partir de cette clé KM_1 recomposée, est classique et identique à celle qui vient d'être décrite précédemment, c'est pourquoi elle n'est pas à nouveau expliquée.

Le procédé de protection d'une clé mère, destinée à permettre l'authentification de cartes utilisateurs, tel qu'il vient d'être décrit s'applique notamment à des systèmes fermés tels les caisses d'un grand magasin, ou alors les machines de jeu d'un casino par exemple. Dans ce cas, il suffit d'introduire la carte superviseur CS, à l'ouverture du magasin ou du casino, dans un serveur apte à recomposer la clé mère KM_1 et à piloter l'ensemble des caisses ou des machines de jeux.

REVENDICATIONS

1. Procédé de protection d'une clé mère (KM_1) destinée à permettre l'authentification de cartes utilisateurs par un lecteur comprenant un module de sécurité (SAM),

caractérisé en ce qu'

- une première partie de la clé mère (KM_{11}) est stockée dans une mémoire du module de sécurité (SAM),

- une deuxième partie de la clé mère (KM_{12}) est stockée dans un support de mémorisation physiquement et géographiquement distinct (CS),

et en ce qu'

- une copie temporaire de la deuxième partie de la clé mère (KM_{12}) est apportée par la carte superviseur (CS) dans une mémoire du module de sécurité (SAM).

2. Procédé selon la revendication 1, en ce que le support de mémorisation est réalisé par une carte à puce superviseur(CS).

3. Procédé selon les revendications 1 ou 2, caractérisé en ce que la première partie de la clé mère (KM_{11}) est stockée dans une mémoire électriquement programmable de type EEPROM du module de sécurité (SAM), et recopiée dans une mémoire volatile de type RAM dudit module de sécurité.

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la deuxième partie de la clé mère (KM_{12}) est stockée dans une mémoire électriquement programmable de type EEPROM de la carte superviseur CS, et sa copie est apportée

dans une mémoire volatile de type RAM du module de sécurité (SAM).

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la totalité de la clé mère (KM_1) est recomposée et stockée dans la mémoire volatile de type RAM du module de sécurité (SAM).

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la clé mère (KM_1) est recomposée sur 8 ou 16 octets.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la copie de la deuxième partie de la clé mère (KM_{12}) est apportée dans la mémoire du module de sécurité (SAM) sous forme cryptée.

8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une deuxième clé mère (KM_2) est stockée en totalité dans une mémoire du module de sécurité (SAM), de manière à permettre l'authentification de la carte superviseur (CS).

9. Procédé selon la revendication 8, caractérisé en ce que la deuxième clé mère (KM_2) est stockée dans une mémoire électriquement programmable et à accès protégé de type EEPROM du module de sécurité (SAM).

FIG_1

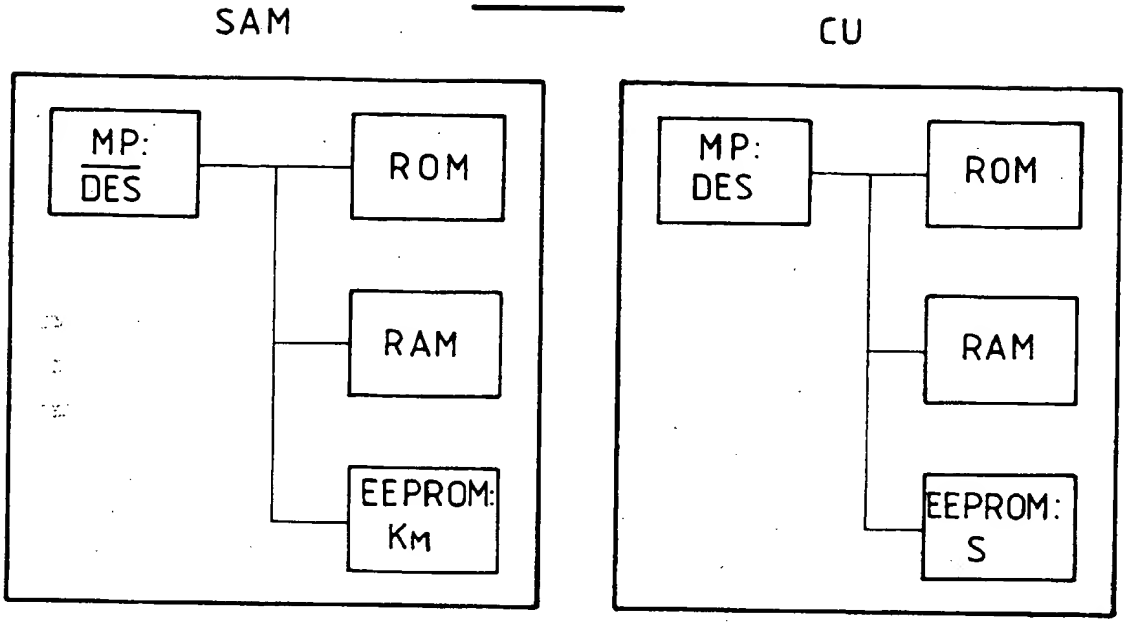


FIG_2

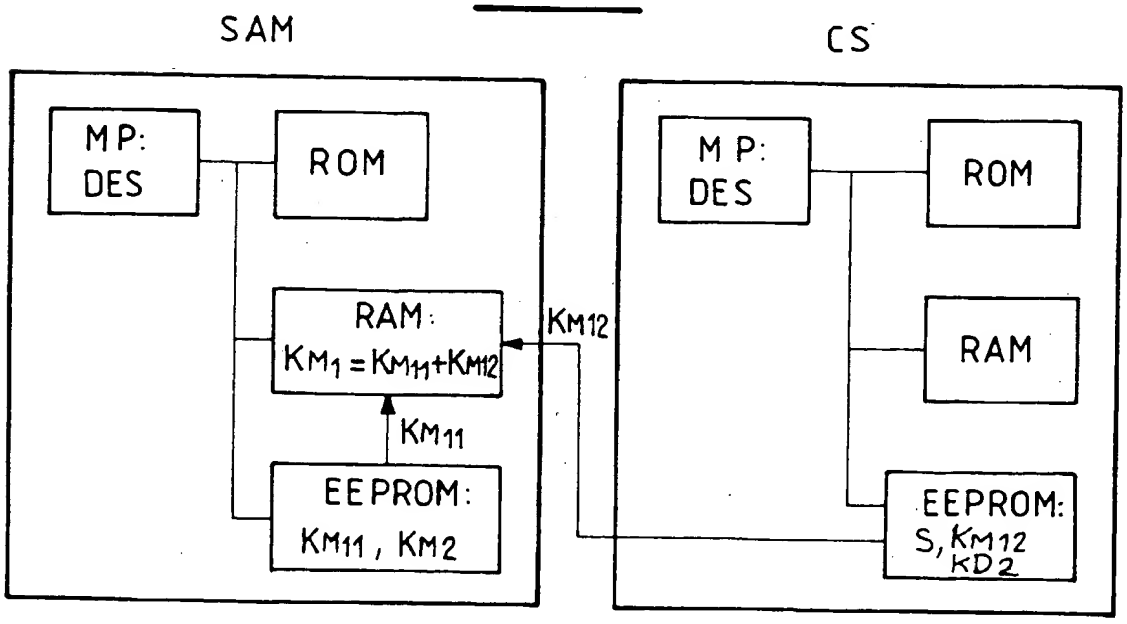
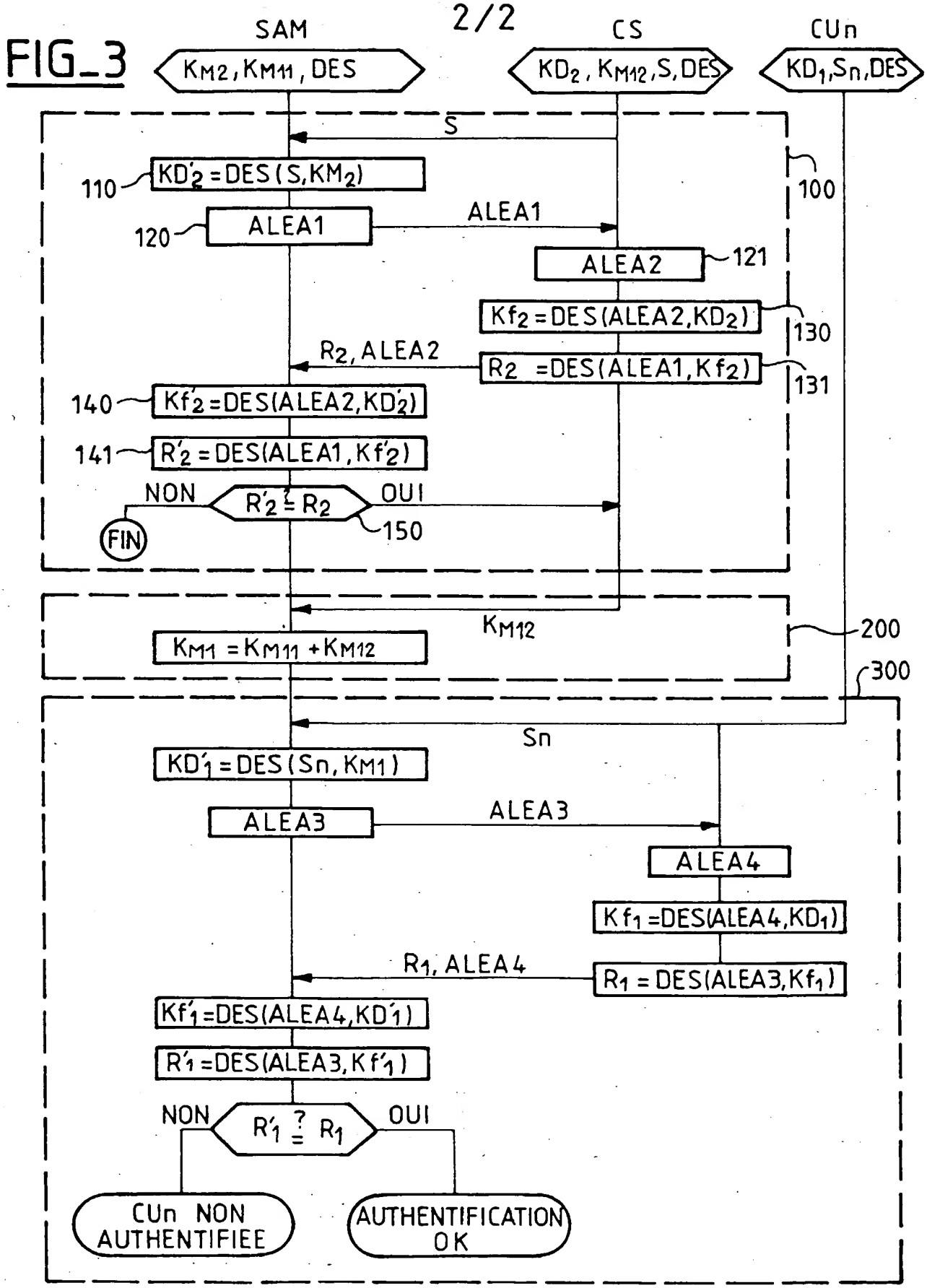


FIG_3



2759833

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 539268
FR 9701965

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y A	EP 0 281 059 A (SIEMENS) * le document en entier *	1-7 8,9
Y	EP 0 355 372 A (SPA SYSPATRONIC) * abrégé; revendications; figures * * colonne 4, ligne 40 - colonne 6, ligne 22 *	1-7
A	EP 0 440 800 A (NTT DATA COMMUNICATIONS SYSTEMS)	
A	EP 0 566 512 A (INNOVATRON TERMINAUX)	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F

Date d'achèvement de la recherche: 15 janvier 1998

Examinateur: David, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)